Massachusetts Institute of Technology

Interim Report of the

Committee on the Changing Nature of Information

March 9, 1983

TABLE OF CONTENTS

PREFACE

There is little question that we are well into an Information Revolution which may affect the world as profoundly as the industrial revolution of the nineteenth century. The associated geo-political and geo-commercial developments have already begun to alter the traditional use, and hence the value, of information in our society. The consequences of these changes are now being felt in the university as the Government seeks to control the dissemination of research results in cryptology and very large scale integration (VLSI) of circuits, and to restrict the participation of foreign scholars in U.S. university research activities.

The forerunners of these developments led the Provost of MIT in October 1980 to establish the MIT Committee on the Changing Nature of Information under the following charge:

The changing nature of information results from the rapid growth of information processing and communications, and in particular of intercommunicating geographically distributed computer systems, and is likely to necessitate new legal, social, and economic approaches for dealing with information. Examples include: (1) privacy and protection criteria that may have to be met before computer data banks become interconnected; (2) the related recent issue of university cryptography research which has important civilian and military repercussions; (3) export control of information; and (4) the consideration of new laws to deal with the changing nature of information. The committee is specifically charged to identify major issues and questions related to the changing nature of information, and to suggest what steps we should take in order to better inform ourselves and others of these issues and their consequences; and to recommend a range of positions for MIT.

The above charge was extended in May 1981 as follows:

The Committee should also address the questions of technology export and participation of foreign students and faculty in research. The context for these questions and the focus of the Committee recommendations should be MIT's research in very large scale integration (VLSI) of solid state circuits, although it should be anticipated that such questions may arise in other research areas as well.

This progress report of the Committee on the Changing Nature of Information has been written to inform the members of the MIT community about relevant issues, and recommended policies along the principal directions of the above charge.

for the Committee,

M.L. Dertouzos, Chairman

1. SUMMARY

This is an interim report of The Committee on the Changing Nature of Information, which was formed by the MIT Provost in October 1980 in order to identify major issues and recommend policies in cryptography and VLSI research. These specific research areas reflect an emerging broader conflict between (1) governmental desires to control the flow of information deemed important to the national security and the international commercial interests of the U.S.; and (2) academic desires to engage freely in research and to communicate without restrictions the fruits of that research.

The historical background relevant to these issues is as follows:

1. In the mid-1970's a conflict emerged between civilian and military cryptology needs through the development of the National Bureau of Standards Data Encryption Standard (DES) which was criticized as being sufficiently difficult to prevent commercial interception but not so difficult as to prevent governmental interception.
2. In 1977 researchers at Stanford and MIT discovered, and publicly disclosed, a "foolproof" encryption scheme whose publication was criticized as possibly violating regulations (International Traffic and Arms Regulations) that control the export of munitions and related technology. Upon determination by our attorneys that these laws were confusing, we continued our research in this area and volunteered to adopt a policy under which papers in cryptology are sent to the National Security Agency (NSA) for their information at the same time that they are sent to our close technical colleagues for comment.
3. In 1978 Professor George Davida of the University of Wisconsin-Milwaukee, who applied for a patent on a cryptographic scheme, was ordered by the Department of Commerce not to discuss or write about his invention. Although the secrecy order was lifted shortly thereafter, it increased the existing controversy.
4. In 1980 at the request of the NSA, the American Council on Education (ACE) established the Public Cryptography Study Group to recommend procedures aimed at easing cryptology research conflicts. The committee developed a set of recommendations based on voluntary prior restraint. At MIT, we reacted negatively to some of these recommendations and declared our preference for our own approach for reasons which are discussed in Section 3.4.
5. In 1981 the National Science Foundation (NSF) amended its policies on research grants, requiring prior restraint on "potentially classifiable research results." MIT, objecting to this language, negotiated with NSF more acceptable language consistent with the relevant Executive Order on classification whereby such prior restraint is invoked only in those extremely rare instances when research results are "believed to require classification."
6. In 1980 the Department of Defense (DOD) established a research program in very high speed integrated circuits (VHSIC) capable of high speed operation in thermally and radioactively hot environments. Concerned about leaks of this new technology to foreign nations, governmental representatives attempted to restrict publication results and the access of foreign scholars to U.S. university research, under Commerce's Export Administration Regulations (EAR). In a letter (Appendix B) to the Secretaries of Commerce, Defense and State, five university presidents, including MIT's Dr. Paul E. Gray, explained how such restrictions would harm one of the principal technological assets of this nation—university research.
7. In January 1982 the "Report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements" was submitted to the Secretary of Defense. This report addressed several issues associated with DOD sponsorship of university research and may have been the first to emphasize the use of the research contract as the focal point for controlling the flow of scientific information.
8. In September 1982 a special panel of the National Academy of Sciences, the National Academy of Engineering and the Institute of Medicine issued its report on "Scientific Communication and National Security." This report, widely known as the Corson Report, sets forth a set of principles aimed at resolving the complex issue that is the subject of our own report, i.e., the conflict between national objectives of scientific communication and national security. We find ourselves in agreement with the principles of the Corson Report but have certain concerns about the way in which these principles may be interpreted or implemented.

The legal framework for governmental controls on technological information includes: (1) The International Traffic in Arms Regulations (ITAR) administered by the Department of State; (2) the Export Administration Regulations (EAR) administered by the Department of Commerce; and (3) Executive Order 12356 on national security. The first two forbid the export without license of munitions, commodities and technical data identified by corresponding lists and associated interpretive instruments. The Executive Order provides for the classification of information, including the results of federally funded research, if disclosure presents a danger to national security. These regulations are complex, bewildering and unclear in their application to scientific and technological research. Moreover, they appear to be impractical for controlling university research. Nevertheless they carry substantial penalties that could have a chilling effect on university research and would result in considerable turmoil if they were to be invoked. Beyond the above three regulations, the Government may decide to use the contractual mechanism as a means for controlling technology transfer: A proposal toward that end is currently under consideration by the Department of Defense. Another potential governmental control stems from the Immigration and Nationality Act which could be used to refuse admission or deport foreign scholars from U.S. research activities.

The issues that emerge from this conflict generally concern research that has basic and applied components, dual civilian and military uses, and commercial repercussions on international competition. Such research is pursued by universities because, as in the case of VLSI, it is inextricably linked to forefront technologies that underlie established academic disciplines; or, as in the case of cryptology, it leads to technologies that are believed to be essential to society in the future.

The Government wishes to control technology leaks in these basic research areas because such leaks may involve national security and economic losses associated with international competition. Such controls generally take the form of prior restraint on publication of research results and restriction of access to U.S. university research by foreign scholars.

Universities object to such controls because they are ineffective, because they impact adversely on the education and training of future scientists and engineers, and because they generally run counter to proven approaches for carrying out academic research. Moreover, constraints on the access of foreign scholars to U.S. university research reduce the size and quality of the U.S. research workforce and are impossible to enforce without creating a discriminatory climate that is incompatible with university traditions. Ultimately, such constraints are perceived by us as reducing our overall scientific and technological leadership and of questionable effectiveness in meeting the Government's objectives.

To strike a balance between the concerns on both sides of this conflict, our Committee recommends an MIT policy which is summarized in Section 6.2 of this report.

2. INTRODUCTION

All of the issues addressed by this report center on the dissemination of information in the context of university instruction and research. Broadly viewed, the conflict that emerges results from the Government's desire to control the flow of information which is deemed important to national security, and the university's desire to pursue freely the generation of new knowledge. To date, MIT has experienced this conflict primarily in two research areas—cryptology, and very large scale integration of solid state circuits.

The factors that have led to this conflict are: (1) the rapidly evolving technology of information processing and communications; (2) the increasing possibilities for dual use of this technology for military and civilian purposes; (3) a decreasing distinction between basic and applied research; and (4) an increased perception that U.S. technology is being exported, thereby weakening this country politically and economically on a world-wide basis.

Our Committee (Appendix A) arrived at its current conclusions through discussions at 23 meetings. Invited guests who were kind enough to express their views before our Committee were Dr. Robert E. Kahn, Director of the Information Processing Techniques Office at the Defense Advanced Research Projects Agency; Dr. Frank Press, President of the National Academy of Sciences; and Mr. Howard Rosenblum, Deputy Director of the National Security Agency. In addition, Committee members attended meetings and contract negotiations with government officials at the NSF, the NSA, and the DOD. Legal counsel was retained in Boston (Mr. Robert Sullivan of Herrick and Smith) and in Washington (Mr. Carl Feldbaum of Palomar Corporation) to analyze the complex laws and regulations surrounding the issues of concern.

This report contains four main sections. A historical survey of developments, especially as they have affected MIT, is presented first (Section 3) in order to explain how we became involved with the relevant issues. Section 4 discusses the framework of current laws and regulations that deal with controls on technological data. Section 5 strives to analyze the crucial issues that emerge in this controversy, and Section 6 presents our Committee's recommendations for an appropriate MIT policy.

3. HISTORICAL BACKGROUND

3.1 The DES Standard

The public concerns over cryptology began in the mid-1970's in connection with the development of the Data Encryption Standard (DES). This standard, set forth by the National Bureau of Standards (NBS) and designed into equipment form by IBM, is intended for the encryption and decryption of digital data primarily in commercial applications. It was developed in order to protect from interception or unwanted modification the increasing amounts of information communicated among interconnected computers. The controversy around this standard evolved from a criticism that DES was carefully selected so as to be sufficiently difficult to prevent commercial interception, but not so difficult as to prevent governmental interception by the National Security Agency. Regardless of the ultimate validity of this criticism, the surrounding publicity was the first significant signal of an emerging conflict between civilian and governmental desires for the protection of data.

3.2 Public Key Cryptosystems and the RSA Algorithm

Shortly after the emergence of the DES criticism, a scientific discovery at Stanford and MIT further increased the civilian/governmental cryptology tension and introduced university research as an important new ingredient of the emerging controversy. This discovery consisted of encryption/decryption schemes developed by Diffie and Hellman of Stanford, called **Public Key Cryptosystems**, and specific encryption/decryption functions for the schemes, developed by Rivest, Shamir and Adleman of MIT, called the **RSA Algorithm**. The combined discovery received a good deal of attention from the popular press and was characterized as putting an end to traditional cryptography. This discovery is important because it allows construction of a code which can be broken only by finding the solution of an extremely complex and time consuming mathematical problem, thereby suggesting that the code is, in effect, unbreakable. Moreover, this approach makes possible not only the **protection** of data being communicated, but also the **authentication** of such data as indeed originating from a legitimate source rather than from an impostor.

The MIT Laboratory for Computer Science (LCS) was in the process of sending out copies of its Technical Memorandum #82 describing the RSA Algorithm, when a new development took place—a letter was written in September 1977 by J.A. Meyer, an NSA employee, who said that he was acting on his own behalf. The letter was addressed to the Information Theory Group of the Institute of Electrical and Electronic Engineers (IEEE). It warned the IEEE scientists (Hellman and Rivest included) who were planning a cryptology symposium for October 1977, that, by holding this symposium and publicly communicating their research results, they might be violating the Department of State's International Traffic in Arms Regulations (ITAR). As explained in Section 4.1 of this report, ITAR controls the flow of military hardware and certain technical data on military technology to foreign countries. According to the Meyer letter, dissemination of such results before a group of foreign scientists who were planning to attend the symposium, or by reprints sent to the Soviet Union, could be regarded as export of technical data controlled by ITAR, and hence as a violation of those regulations.

The cryptology symposium discussed above did take place, after some changes were made in the presentations to limit discussion to mathematical issues. At MIT/LCS, as a result of the Meyer letter, we stopped dissemination of Technical Memorandum #82, pending determination of the legality of its publication by our attorneys. We soon found out that there was no clear legal answer to this question. In particular, the laws and regulations surrounding ITAR appeared to be overly complex and bewildering. Strict interpretation of their language would yield the absurd conclusion that these regulations had been violated by industry and academia for many years. Yet there were hardly any legal precedents governing such violations and our lawyers felt that strict enforcement of the applicable regulations would most likely be viewed by the courts as unconstitutional. This opinion was to be later reinforced by a memorandum prepared by the U.S. Department of Justice for the Science Advisor to the President.

To understand better the governmental views on these regulations, and to alert the Government to our views on the future importance of public cryptography (see Section 5.1), we initiated two meetings. One, at MIT, was with the President's Science Advisor, Dr. Press; the Deputy Undersecretary of Defense in charge of Intelligence, Dr. Dineen; the Deputy Director of the NSA, Mr. Rosenblum; and the Director of MIT/LCS, Prof. Dertouzos. The other meeting was a visit of Professors Rivest and Dertouzos with Mr. Rosenblum at the NSA. These meetings, five years ago, reinforced our views on the murkiness of ITAR and left us with a feeling that the Government did not fully share our concerns on the future evolution of the information field. Nevertheless, there was a willingness on both sides to try to find a workable scheme that would protect our mutual interests. To that end, MIT proposed at one of these meetings an approach that was later to become part of our recommended MIT policy in cryptology. Under this approach, the MIT/LCS, as the locus of cryptology research at MIT, volunteered to send all cryptology papers to the NSA at the same time that they are sent to the author's close colleagues for technical comment. In proposing this scheme, we made clear our intent that these papers would be sent to the NSA **for their information** and not for securing their permission to publish.

Shortly after these meetings, in the absence of any clear answer to our questions on legality, and in view of our volunteered action, we informed the DOD that we were resuming publication of LCS Technical Memorandum #82.

3.3 The Davida Secrecy Order

In early 1978 George I. Davida, Professor of Computer Science at the University of Wisconsin-Milwaukee, applied for a patent on a novel cryptographic scheme. In April 1978 he received a letter from the Department of Commerce which ordered him not to discuss or write about the principles in this cryptographic scheme. This invocation of a patent secrecy order by Commerce under the Invention Secrecy Act raised considerable objections in the academic community, notably from Wisconsin's Chancellor Werner Baum who, according to *Science* (July 14, 1978), was outraged at what he regarded as an invasion of his faculty's academic freedom without due process.

The secrecy order was lifted shortly thereafter and, as in prior incidents, the main crisis was averted while the surrounding discussion served to increase awareness and concerns about the possibility of more serious conflicts between the university and government.

3.4 The ACE Public Cryptography Study Group

In March 1980, in response to a request by the NSA, the American Council on Education (ACE)—a group of university administrators—established a Public Cryptography Study Group. The NSA's concern that led to formation of this group was expressed by Vice Admiral Bobby Inman, Director of the Agency, who felt that information contained in published articles and monographs on cryptography endangered the national security.

The group, after meeting for a year, recommended a voluntary prior restraint procedure under the following guidelines:

1. *NSA would notify the cryptologic community, including authors and publishers, of its desire to review manuscripts concerning aspects of cryptology prior to publication.*
2. *NSA, in consultation with appropriate technical societies, would define as precisely as possible those aspects of cryptology to be covered by the procedure.*
3. *NSA would invite authors to send manuscripts to NSA for review prior to publication.*
4. *NSA would assure prompt review by its staff of submitted manuscripts and prompt response to authors with an explanation, to the extent feasible, of proposed changes, deletions, or delays in publication, if any.*
5. *NSA would provide, in the case of unresolved disagreements, the opportunity for authors to obtain prompt review by an Advisory Committee of five persons (two appointed by the Director of NSA and three appointed by the Science Advisor to the President from a list of nominees provided by the President of the National Academy of Science), which would make a recommendation to the Director of NSA and to the author concerning the matters in issue. Members of the Advisory Committee shall have adequate clearance so that the committee can make informed recommendations.*
6. *There would be a clear understanding that submission to the process is voluntary and neither authors nor publishers will be required to comply with suggestions or restrictions urged by NSA.*

At MIT, we reacted negatively to some of these recommendations and declared our preference for our own approach for the following reasons:

1. *Under the ACE scheme, researchers carry the burden of deciding what papers to submit to the NSA for review. Under the MIT scheme, all papers in cryptology are submitted, thereby relieving the researcher from decisions that necessarily must be based on partial knowledge as to what may or may not require classification.*
2. *A researcher who adheres to the ACE scheme accepts restraints prior to the publication of research results. The MIT scheme does not involve prior restraint.*
3. *Even though it is voluntary, the ACE scheme may be viewed as practically obligating researchers to comply. Moreover, several researchers felt that the voluntary aspect of the ACE scheme was a test and a first step toward eventual formalization of prior restraint on a non-voluntary basis.*

3.5 The NSF Policy Changes

In August 1980, the National Science Foundation (NSF), at NSA's prodding, told MIT computer scientist Leonard Adleman (then on leave at the University of Southern California), that parts of his NSF cryptology research grant proposal would not be funded. We believe that this was the first instance in NSF's grant history that funds were refused for reasons of national security. At the same time, Professor Rivest of MIT was also notified by the NSF that his pending proposal would probably meet with the same fate.

Subsequently, Adleman received a call from Admiral Inman who indicated that the NSA wanted to fund his proposal. The offer was refused by Adleman who was concerned about accepting funds from the NSA when he had applied to the NSF. Eventually, NSF granted Adleman the entire sum that he had requested, but included language in the grant letter that in effect made Adleman responsible for seeking prior restraint.

The NSF difficulties in cryptology research reappeared later in mid-1981 in connection with the Rivest proposal. Prior to that time, the NSF had established a subcommittee, under the leadership of Professor John Guttag of MIT, to recommend NSF policy changes for dealing with cryptology research. The Guttag report recommended a scheme similar to that adopted by MIT for informing the NSA of relevant research results. Subsequently, the NSF notified MIT of changes in its grants policy which, in opposition to its own subcommittee recommendations, required a prepublication review. The new language in Section 794C of the NSF Grant Policy Manual was as follows:

When in the course of an NSF supported project information or materials are developed which may affect the defense and security of the United States, the grantee: (i) has the responsibility to notify immediately the cognizant NSF program Director of any data, information or materials developed under an NSF-supported project which may require classification; (ii) shall prior to dissemination, distribution or publication of the potentially classifiable research results allow NSF the option of reviewing such materials; (iii) shall, upon receipt of notice from the cognizant NSF Program Director of NSF's intention to exercise its option, defer dissemination, distribution, or publication pending exercise by NSF of its option of review and determination that the results are not classified, and when requested by the NSF Program Director, direct the potentially classifiable materials to the NSF Security Officer, 1800 G St., N.W., Washington, D.C., 20550. Provided further, however, that such deferral is subject to NSF's review and determination being completed within 60 days of receipt by NSF of such material.

We objected to this language primarily because it imposes prior restraint on **potentially classifiable** research results—an ominous phrase which would apply not only to cryptology but to **all** NSF supported research.

The language that was finally negotiated between NSF and MIT for the Rivest grant was based on the exact language of Presidential Executive Order 12065, (the precursor of the Executive Order discussed in Section 4.4) and was as follows:

In those rare instances when data, information, or materials developed in the course of a project supported by NSF are believed to require classification, the grantee: (i) has the responsibility to notify immediately the cognizant NSF Program Director; (ii) shall, prior to dissemination, distribution, or publication of such data, information, or materials allow NSF the option of reviewing them; (iii) shall, upon receipt of notice from the cognizant NSF Program Director of NSF's intention to exercise its option, defer dissemination, distribution, or publication pending exercise by NSF of its option of review and determination by the appropriate agency that the materials are not classifiable; and when requested by the NSF Program Director, direct the potentially classifiable materials to the NSF Security Officer, 1800 G Street, N.W., Washington, D.C. 20550. Provided further, however, that such deferral is subject to review and determination being completed within sixty (60) days of receipt by NSF of such materials.

We agreed to this language because it was essentially identical to the language of the Executive Order on classification and because of the extreme improbability that it would be invoked.

We subsequently asked the NSF to clarify whether the revised language would apply to all NSF grants as we had understood during our negotiations, or only to the Rivest grant. The NSF has not, as of this writing, responded to our request, leaving ambiguous the range of applicability of the old and new clauses.

3.6 Very Large Scale Integrated (VLSI) Circuit Research

Two factors seem to be at the root of the next development: The first is the progressively increasing involvement of U.S. universities in VLSI research, primarily because of the maturation of the associated design and process technologies. The second involves the Department of Defense's desire in 1980 to establish a research and development program for very high speed integrated circuits (VHSIC—pronounced vis-ick)—a subclass of very fast VLSI circuits capable of working in thermally and radioactively hot environments for use in the control and instrumentation of weapons. These factors led to questions about the participation of foreign students and faculty in VLSI research and the export of technical data concerning weapons technology. In addition to the ITAR-based concerns, these developments brought into focus the Department of Commerce's Export Administration Regulations (EAR). The EAR, discussed in Section 4.3, are intended to control the export of critical technologies with dual military and civilian uses. Finally, it seems that several people within government began to be progressively more concerned with the economic advantage afforded foreign nations, notably Japan, through easy export of our forefront technologies.

These governmental concerns, which were reflected in discussions with universities about contractual arrangements for VLSI research, along with incidents involving restrictions of foreign scientists at Cornell and MIT, led to substantial and negative academic reactions. The culmination of these academic concerns was a letter signed by the five presidents of California Institute of Technology, Cornell, MIT, Stanford, and the University of California, which was sent in February 1981 to the Secretaries of Commerce, Defense, and State (Appendix B). This letter made the case that the contemplated restrictive measures would harm one of the principal technological assets of this nation—university research. The five presidents did eventually receive replies from all three secretaries who tried to reassure the academic community that such controls would not be carelessly invoked. Nevertheless, the academic community remained and still remains unsure of what constraints, if any, would be imposed by the Government on the conduct of such research.

Concerns about academic research were once again raised in January 1982 by Deputy Secretary of Defense, Frank Carlucci; Deputy Director of the CIA, Bobby Inman; and Secretary of Defense, Caspar Weinberger. Carlucci set forth in *Science* (January 8, 1982) examples of Soviet scientists who, after working in U.S. universities, return to weapons development in the USSR, and of USSR exploitations of senior-scholar exchanges, whereby Soviet scientists interested in military applications of research are proposed, while we propose scholars interested in the humanities. Inman, speaking before the American Association for the Advancement of Science (AAAS) meeting of January 7, 1982, called for prepublication review of university research results in cryptography, computer hardware and software, lasers, crop projections and manufacturing processes. Weinberger stated that the Soviets "have organized a massive, systematic effort to get advanced technology from the West."

As of the writing of this report, there has been no resolution of these more recent issues involving the prepublication review of results, and the participation of foreign scholars in critical university research areas.

3.7 The Report of the Defense Science Board Task Force

In January 1982 the "Report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements" was submitted to the Secretary of Defense through the Office of the Under Secretary of Defense for Research and Engineering. This report was prepared in response to a House Armed Services Committee request and addressed several issues associated with DOD sponsorship of university research.

With respect to export control, the flavor of the report is captured by the following two excerpts:

DOD is caught in a dilemma. If it vigorously attempts to regulate the flow of scientific information in the scientific community, it could jeopardize the strength and vitality of the very community it is seeking to revitalize for the sake of national defense. On the other hand, if DOD abandons any attempt at regulation in the university context, it could seriously compromise and, in certain cases, totally undercut other efforts to control the out-flow of militarily critical technology. The middle ground is a difficult one to establish. This Task Force has attempted, if not to solve the problem, to at least lay a framework for solving the issue by means both practicable and, it is hoped, acceptable to the academic community. A dialogue with the universities has already begun over the transfer of non-classified but nonetheless sensitive information in the Very High Speed Integrated Circuit (VHSIC) Program.

The focal point for control is the DOD contract: the Government negotiates the terms of the release of information with the contractor. The Project Office or Contract Monitor within DOD thus becomes the interpreter of military criticality and the extent to which ITAR or EAR is applicable. The system is voluntary in the sense that the contract does not have to be accepted. If guidelines for release of information are accepted as part of the contract, then there should be little room for misunderstanding later. It could be argued that restrictions such as these violate the spirit of academic freedom and will curtail the free flow of information required for maintaining a healthy dialogue within the scientific community. This might be true if DOD were seeking to restrict the flow of all scientific information directly or indirectly related to military capability. This, however, is clearly not the case. The Department of Defense is assiduously rejecting any control guidelines that would restrain the development and dissemination of the fruits of basic research.

This report may have been the first to emphasize the use of the research contract as the instrument of control, rather than placing reliance upon more generalized devices such as ITAR or EAR.

3.8 The Corson Report

In September 1982, an important report entitled "Scientific Communication and National Security" was issued by the Panel on Scientific Communication and National Security of the Committee on Science, Engineering and Public Policy of the National Academy of Sciences, the National Academy of Engineering and the Institute of Medicine. This document, known as the **Corson Report** after the Panel's Chairman Dale R. Corson, sets forth a set of principles aimed at resolving the complex issue that is the subject of our own report, i.e., the conflict between the national objectives of scientific communication and national security.

The Corson Report discusses: (1) the unwanted transfer of militarily significant U.S. technology to the Soviet Union; (2) the importance of openness for the principal mission of U.S. universities; (3) the current control system; and (4) the costs and benefits of these controls. The key recommendations of the Corson Report are:

1. On the control of university research activities, the panel identifies three categories of research—clearly open, clearly classified and a small "gray area" for which limited restrictions short of classification are appropriate. In the language of the Corson Report:
   The Panel recommends that no restriction of any kind limiting access or communication should be applied to any area of university research, be it basic or applied, unless it involves a technology meeting all the following criteria:
   - *The technology is developing rapidly, and the time from basic science to application is short;*
   - *The technology has identifiable direct military applications; or it is dual-use and involves process or production-related techniques;*
   - *Transfer of the technology would give the U.S.S.R. a significant near-term military benefit; and*
   - *The U.S. is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours.*

   The panel recommends that in the limited number of instances in which all of the above four criteria are met but classification is unwarranted, the values of open science can be preserved and the needs of government can be met by written agreements no more restrictive than the following:
   a) Prohibition of direct participation in government-supported research projects by nationals of designated foreign countries with no attempt made to limit physical access to university space or facilities or enrollment in any classroom course of study. Where such prohibition has been imposed by visa or contractually agreed upon, it is not inappropriate for government-university contracts to permit the government to ask a university to report those instances coming to the university's attention in which the stipulated foreign nationals seek participation in any such activities, however supported. It is recognized that some universities will regard such reporting requests as objectionable. Such requests, however, should not require surveillance or monitoring of foreign nationals by the universities.
   b) Submission of stipulated manuscripts simultaneously to the publisher and to the federal agency contract officer, with the federal agency then having 60 days to seek modifications in the manuscript. The review period is not intended to give the government the power to order changes: The right and freedom to publish remain with the university, as they do with all unclassified research. This does not, of course, detract from the government's ultimate power to classify in accordance with law any research it has supported.
   The panel recommends that in cases where the government places such restrictions on scientific communication through contracts or other written agreements, it should be obligated to record and tabulate the instances of those restrictions on a regular basis.
   The provisions of EAR and ITAR should not be invoked to deal with gray areas in government-funded university research.
2. On the export of domestically available technical data under EAR and ITAR:
   1. The Panel recommends that unclassified information that is available domestically should receive a general license (exemption) from the formal licensing process.
   2. The Panel recommends that information that is not directly or significantly connected with technology critical to national security should also receive a general license (exemption) from the formal licensing process. The critical technology list approach—if carefully formulated—could serve to define those limited areas in which controls are appropriate.
3. On the use of voluntary controls:
   The Panel concludes that the voluntary publication control mechanism developed for cryptography is unlikely to be applicable to other research areas that bear on national security. However, the Panel recommends that consideration be given to adopting this mechanism in future cases, if and where the appropriate preconditions exist.
4. On the Militarily Critical Technologies List (MCTL):
   The Panel recommends a drastic streamlining of the MCTL by reducing its overall size to concentrate on technologies that are truly critical to national security.
5. Finally, on technology transfer to the third world, the panel reached no conclusions and recommended further study.

In the above summary we have emphasized, through inclusion of more extensive quotations, the Corson Report recommendation on the control of university research activities because we comment on it further in Section 6.3 of this report.

4. THE LEGAL FRAMEWORK

4.1 Introduction

The control of technological information by the U.S. Government falls under one of the following principal categories of laws and regulations:

1. The Arms Control and Export Act of 1976 (ITAR)
2. The Export Administration Act of 1979 (EAR)
3. The Executive Order on National Security Information.

These are discussed in more detail in the three subsections that follow.

In addition, there is: (1) the Atomic Energy Act of 1954 which established the "born secret" concept, i.e., the notion that new results or even unclassified material presented in a new way can be called classified; (2) the Invention Secrecy Act (1951) which permits the classification of patents involving national security; (3) the Freedom of Information Act which contains provisions for exempting agencies from having to disclose certain types of information; (4) the Executive Order on Intelligence (December 1981) which allows for the covert collection of information by aqents posing as journalists or academics; and (5) various scientific and cultural exchanges with respect to which the Department of State places restrictions on foreign visitors. These five vehicles are tangential to our concerns and will not be discussed further. They may, however, assume renewed importance as new developments emerge.

Finally, there are two potentially significant ways in which the Government could exercise control over the export of technological information—the research contract and the Immigration and Nationality Act which we discuss in Section 4.5.

4.2 The Arms Control and Export Act of 1976 (ITAR)

The International Traffic in Arms Regulations (ITAR) has been formulated by the Department of State to implement the Arms Control and Export Act.

Under the ITAR, all non-exempt equipment listed in the **United States Munitions List** as "arms, ammunition and implements of war," as well as

related classified and unclassified technical **data**, may not be exported except under a license issued by the Office of Munitions Control of the State Department. The ITAR definition of "export" is broad, particularly with respect to the export of technical data:

*The export controls of this subchapter shall apply whenever the information is to be exported by oral, visual or documentary means. Therefore, an export occurs whenever technical data is, **inter alia**, mailed or shipped outside the United States, carried by hand outside the United States, disclosed through visits abroad by American citizens (including participation in briefings and symposia) and disclosed to foreign nationals in the United States (including participation in briefings and symposia).*

The Office of Munitions Control, in Munitions Control Newsletter No. 80 (February 1980), has further clarified and limited the ITAR's licensing provisions as applied to unclassified cryptologic technical data. As that newsletter states:

Cryptologic technical data for which a license is required under Section 121.01, Category XVIII, is interpreted by this office with respect to information relating to Munitions List items in Categories XI (c) and XIII (b) to include only such information as is designed or intended to be used, or which reasonably could be expected to be given direct application, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction of items in such categories. This interpretation includes, in addition to engineering and design data, information designed or reasonably expected to be used to make such equipment more effective, such as encoding or enciphering techniques and systems, and communications or signal security techniques and guidelines, as well as other cryptographic and cryptanalytic methods and procedures. It does not include general mathematical, engineering or statistical information, not purporting to have or reasonably expected to be given direct application to equipment in such categories. It does not include basic theoretical research data. It does, however, include algorithms and other procedures purporting to have advanced cryptologic application.

The United States Court of Appeals for the Ninth Circuit has limited substantially the scope of the ITAR. According to that Court, the ITAR "prohibits only the exportation of technical data significantly and directly related to specific articles on the Munitions List" and, in circumstances where the data could have both military and peaceful applications, such prohibition is enforceable only to the extent that the exporter knows—or has reason to know—that the information is intended for the prohibited (military) use. (*United States v. Edler Industries, Inc.*)

Unlicensed export of materials or data included on the Munitions List—if "willful"—can result in fines of up to $100,000 and/or imprisonment for up to two years. The Act provides for civil penalties as well.

The ITAR must be viewed as an imperfect tool for restricting the transfer of "technical data." Its infirmities may well explain the NSA efforts to construct, through dialogue, the informal mechanism recommended by the ACE Committee. The problems of ITAR are as follows:

First, no one really knows what the definition of "technical data" encompasses and how it might specifically apply to cryptological information. The difficulty of clarifying this definition is exemplified by the Department of State's interpretive newsletter (Newsletter No. 80) which asserts that "technical data" does not include mathematical concepts, but includes certain algorithms—a technically ineffective partition since the transition from a basic theory to an algorithm is often a straightforward process.

Second, the ITAR has no application to information in the public domain. Thus, publication in *Science* or *Scientific American* not only disseminates the information, it effectively removes ITAR's application to the published information.

Third, as already discussed, the leading legal precedent, *U.S. vs. Edler Industries*, reads into ITAR a **scienter** requirement, meaning that the person disclosing the information to a foreign national must do so with knowledge or reason to know that the foreign national intends to use the information in a prohibited end use—an intention probably absent and difficult to prove in the academic environment.

Finally, the Department of Justice itself has raised serious concerns about the constitutionality of ITAR on the grounds that it operates as a prior restraint on free speech without the usual safeguards of judicial review.

4.3 The Export Administration Act of 1979 (EAR)

In an attempt to clarify uncertainties in United States export control policies and to utilize such policies in furtherance of national security, foreign policy and economic objectives, Congress enacted the Export Administration Act of 1979, replacing the Export Administration Act of 1969.

Acting under this authority, the Department of Commerce has issued a lengthy series of Export Administration Regulations (EAR). Exports subject to licensing under the EAR—including specified commodities and related technical data—require approval from the Office of Export Administration, Department of Commerce, in the form of a license.

The defense articles and defense services on the U.S. Munitions List are expressly excluded from the EAR licensing framework. Nevertheless, included among the list of commodities for which a validated export license is required are:

Cryptographic equipment and ancillary equipment (such as teleprinters, perforators, vocoders, visual display units) designed to ensure secrecy of communications (such as telegraphy, telephony, facsimile, video, data) or of stored information, their specialized components; and software controlling or performing the function of such cryptographic equipment. Also video systems which, for secrecy purposes, use digital techniques (conversion of an analog, i.e., video or facsimile, signal into a digital signal). (This item also covers digital computers and differential analyzers (incremental computers) designed or modified for, or combined with, any cipher machines, cryptographic equipment, devices or techniques including software, micro-program (hardware), associated equipment therefor, and equipment or systems incorporating such computers or analyzers), except simple cryptographic devices or equipment only ensuring the privacy of communications.

Assuming that certain cryptographic equipment falls outside of Department of State jurisdiction but within the purview of the EAR, the Commodity Control List indicates that such equipment may not be exported to any nation except Canada without a license. Further, the list indicates that the reason for control of such equipment is national security. This being the case, the Secretary of Defense is authorized to review any proposed export of such equipment or related technology for the purpose of determining whether such export would "make any contribution, which would prove detrimental to the national security of the United States, to the military potential of such [foreign] country or any other country."

Technical data is treated as distinct from commodities under the EAR, and is regulated in depth. The relevant section defines technical data as follows:

"Technical data" means information of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization, or reconstruction of articles or materials. The data may take a tangible form, such as a model, prototype, blueprint, or an operating manual; or they may take an intangible form such as technical service.

The definition of what constitutes an "export" of such data is as broad as that contained in the ITAR. Three categories are identified:

(1) "Export of Technical Data" means —(i) An actual shipment or transmission of technical data out of the United States; (ii) Any release of technical data in the United States with the knowledge or intent that the data will be shipped or transmitted from the United States to a foreign country; or (iii) Any release of technical data of U.S. origin in a foreign country.

(2) Reexport of technical data. "Reexport of technical data" means an actual shipment or transmission from one foreign country to another, or any release of technical data of U.S. origin in a foreign country with the knowledge or intent that the data will be shipped or transmitted to another foreign country. Technical data may be released for reexport through: (1) visual inspection of U.S.-origin equipment and facilities abroad; (2) oral exchanges of information abroad; and (3) the application to situations abroad of personal knowledge or technical experience acquired in the United States.

There is a so-called "General License" —that is, a license granted automatically by EAR without the need of application —for technical data falling in the following categories:

(a) Data generally available. Data that have been made generally available to the public in any form, including: (1) Data released orally or visually at open conferences, lectures, trade shows, or other media open to the public; and (2) publications that may be purchased without restrictions at a nominal cost or obtained without cost or are readily available at libraries open to the public. The term "nominal cost" as used in paragraph (a) (2) of this section is intended to reflect realistically only the cost of preparing and distributing the publication and not the intrinsic value of the technical data. If the cost is such as to prevent the technical data from being generally available to the public, General License GTDA would not be applicable.

(b) Scientific or educational data. (1) Dissemination of information not directly and significantly related to design, production, or utilization in industrial processes, including such dissemination by correspondence, attendance at, or participation in, meetings; or (2) Instruction in academic institutions and academic laboratories, excluding information that involves research under contract related directly and significantly to design, production, or utilization in industrial processes.

(c) Patent applications. Data contained in a patent application prepared wholly from foreign-origin technical data where such application is being sent to the foreign inventor to be executed and returned to the United States for subsequent filing in the U.S. Patent and Trademark Office. (No validated export license from the Office of Export Administration is required for data contained in a patent application, or an amendment, modification, supplement or division thereof for filing in a foreign country in accordance with the regulations of the Patent and Trademark Office in 37 CFR Part 5. See § 370.10(j).)

Willful violations of the EAR licensing provisions can result in fines up to $50,000 and imprisonment for up to five years. There is no reported case law interpreting the technical data provision of the EAR.

A working group is currently drafting a new list of Military Critical Technologies which is expected to be rather broad in its coverage, and a new set of regulations has been drafted but has been stalled, at least for the time being, because of negative reactions by the scientific community.

4.4 Executive Order 12356 on National Security Information

On April 2, 1982, President Reagan signed Executive Order No. 12356 replacing Executive Order No. 12065 which had been promulgated by the Carter Administration. The new Order reverses many of the presumptions of the prior Order and in general makes classification easier. In its draft form, the new Order had eliminated the exception according to which "basic scientific research information not clearly related to the national security may not be classified." This exception was eventually reinstated and now appears in the current Executive Order following vigorous opposition to its elimination by the academic community, led by MIT President Paul E. Gray.

The complete scope of the new Executive Order is not clear. By its terms, it extends to all information that is "owned by, produced by or for, or is under the control of the United States Government". Informal interpretations include all work sponsored by the federal government. (There is some concern that the new Order's elimination of an exception for private sector research can be read as a signal that the new Order extends to private sector research, but any such intention has been informally denied by the Administration.)

The most important new provision affecting universities is Section 1.2(e) which provides:

1-205. Exceptional Cases. When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

The obligation placed upon a contractor or grantee originating information to safeguard that information under this section is uncertain since it requires formation of a "belief" that the information requires classification. (See also Section 3.5 for the MIT-NSF agreement which involves this requirement.) Another portion of the Order (1.1(c)) augments the problem with the provision "if there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority..." It would be open to the Government to contend that safeguarding is required if the grantee has reasonable doubt about the need to classify.

If information is classified, it may not, under penalty of criminal sanction, be disclosed to anyone without governmen-

tal clearance. The restriction is absolute.

Finally, unlike the ITAR which restricts "export of information to foreign nationals", classification restricts disclosure of information to anyone.

4.5 Contract Terms and the Immigration and Nationality Act

In addition to the above laws, there is evidence that the Government is considering the use of contract and grant terms in federally sponsored research as a means of controlling the dissemination of research results. Such restrictions entered into voluntarily by grant recipients and contractors may avoid the constitutional doubts surrounding ITAR and EAR and may become the most effective means for controlling the flow of scientific information. The Defense Science Board Task Force on University Responsiveness has suggested (see Section 3.7), and the Department of Defense is reportedly considering, a mechanism which would focus control of research results on the negotiation process at the time of the government grant or contract.

Another potential controlling mechanism may evolve from the Immigration and Nationality Act which empowers the Government to refuse admission to an alien if there is reason to believe that the alien will "engage in activities which would...endanger the welfare, safety, or security of the United States." In addition, an alien may be deported for failing to comply with the conditions under which he was admitted. To date, the immigration laws have not been used in any general way to control technology transfer. Recently, however, the Department of State has made formal inquiries to universities of the intended areas of research of certain foreign nationals from Communist countries.

4.6 Interpretation and Conclusions

As is evident from the above summaries of the relevant laws and regulations, the legal structure surrounding the control of scientific and technological information is bewildering. Nevertheless, we shall attempt to draw several conclusions.

The regulations appear to be impractical instruments not intended to regulate scientific exchange in the academic world, for the following reasons:

1. At least ITAR and EAR exclude basic research from their sphere of control.
2. The scienter requirement of the Edler case—that the person disclosing information know that the recipient of the information intends to use it for a prohibited purpose in a foreign country—provides a legal precedent for a similar requirement for EAR.
3. Neither EAR nor ITAR can control information which has already reached the public domain. Thus the Government would find it difficult to prosecute a case where the information disclosed in a meeting had already appeared in some generally available publication.
4. Serious questions have been raised by the Department of Justice about the constitutionality of both the ITAR and the EAR in their present form.
5. It is believed that, to date, no university has applied for a license under the EAR.

Ultimately, we cannot conclude that we should be at ease about the implications of these regulations. On the contrary, the mere commencement of a criminal proceeding by State or Commerce would create confusion and doubt and would have a chilling effect on our researchers. Moreover it would take the courts several years to make rulings on some of these issues.

Accordingly, we believe that our best approach is to maintain an ongoing dialogue with the Government for a bilateral exposition of views, issues and concerns; and to initiate a range of MIT policies that address these problems in responsible and effective ways.

5. ISSUES

5.1 Critical Technologies

For the purposes of this report we may regard university research activities as points within a cube, whose dimensions are: (1) basic to applied; (2) civilian to military; and (3) internationally non-competitive to competitive. At one extreme, basic research of only civilian interest with no potential for international competition presents no conflict and can be freely pursued at the university. Equally clearly, research at the opposite extreme does not belong in a university and most probably should be classified. The concerns addressed by this report involve research on so-called **critical or sensitive technologies** located somewhere in the middle of this cube, i.e., having basic and applied components, dual military-civilian uses, and international competitive interest. This is indeed the case with both cryptology and VLSI research.

Starting with cryptology, we foresee that during the next decade there will be a progressively increasing number of interconnected computers communicating both within and across organizational boundaries. Conceivably, if personal computers continue to grow at their current rate of some one million new units/year the aggregate of geographically distributed systems will extend to individual homes and small businesses as well. In such a future setting we believe that the protection and authentication of data is a mandatory requirement. Recall that by protection we mean that data may be communicated without interception, whereas by authentication we mean the existence of credible means for certifying the signatory of an electronic message.

Data must be protected precisely because the power of computers makes possible the malicious use of these machines in breaking the defenses of a remote installation, selecting data of interest, copying it and finally erasing all traces of such an invasion. As the use of geographically distributed interconnected systems grows beyond today's banking and business applications to broader financial, legal, medical and governmental services the potential and penalty for such misuses becomes greater. It is for this reason that we assert a societal need for vigorous research in public cryptology. For it is only through cryptologic techniques that the protection and authentication of data can be effectively insured.

In addition, the unconstrained pursuit of cryptologic research is expected to have beneficial intellectual repercussions in allied fields of computer science. More importantly the timing of expected developments strongly suggests that **now** is the time to pursue effectively such research and thus to gain on the frontiers of theoretical computer science knowledge. The above motivations are unfortunately in conflict with the possible damage that new publicly available cryptologic results can cause in governmental communications and in the acquisition of foreign intelligence.

Proceeding to our second major area, we believe that VLSI research is instrumental to the future evolution of the electrical engineering and computer science disciplines. More specifically, progress in the formation of new systems depends critically on the structure and function of their subordinate components—which are VLSI circuits. Thus, for example, the development of successful speech-comprehension systems appears to depend critically on the design of proper VLSI structures that will be used in large numbers to carry out simultaneously and in parallel many similar information processing operations.

If automatic speech comprehension is achieved, it will have, besides the obvious civilian and military applications, international competitive repercussions. Japan, for example, has already embarked on a ten-year project to achieve this goal (the Fifth Generation Computer Project) with the express intent of eventually dominating the world's computer markets. As before, we see here the presence of a commercial conflict, which becomes particularly important in VLSI, because circuits can be easily copied and replicated.

The same argument is applicable to VLSI design techniques, an area where U.S. dominance is expected. In this area, we are concerned with computer-based techniques for effectively designing very small VLSI circuits (e.g., five mm. on each side) containing over 100,000 circuits—a design process that cannot be carried out manually because of inherent complexities. A successful system capable of such design complexity, along with its software components, can be easily copied, perhaps by foreign scholars who participate in this research.

The conflicts of purpose characterized by these examples are further compounded by a confusion of boundaries: In both cryptologic and VLSI research the boundary between what is basic research of civilian interest and what can be used for military or international competitive purposes is very diffuse. Consider, for example the RSA encryption scheme discussed in Section 3.2. That scheme can be viewed as: (1) a mathematical theory that defines certain functions; (2) an algorithm that implements these functions using subordinate functions like multiplication; and (3) one or two VLSI circuits that implement in hardware that algorithm. Here, the creative and most difficult part has been the discovery of the theory—a basic research activity. The conversion of this theory to an algorithm and the subsequent conversion of that algorithm to VLSI circuits are relatively straightforward development activities that can be effectively carried out by any good team of domestic or foreign engineers. Can this research activity be clearly partitioned into non-critical and critical parts?

In conclusion, certain new research activities are by their very nature multifaceted, i.e., they have basic and applied components, and are significant in the international commercial and military arena. The pursuit of such research is essential for the fundamental growth and leadership of U.S. technology, yet the easy "export" of this research is believed undesirable for it may tend to weaken the nation in military and commercial terms.

5.2 The Problems of Technology Export

The export of technology that is the focus of governmental concerns involves the leakage of university research either (1) in the form of research results; or (2) through the training of foreign scholars in critical technologies on U.S. campuses. In cryptology, the NSA is charged with the responsibility of (1) insuring the security of governmental communications; and (2) gathering intelligence from foreign communications. These two pursuits have the technically conflicting objectives of desiring good cryptography for the U.S. and bad cryptography for other countries. Thus, public cryptology work, if successful, usually helps one of these objectives while hindering the other, depending on whether it enables better code-making or better code-breaking.

The financial costs to our Government of the disclosure of critical code-breaking techniques can be measured in billions of dollars. For example, the NSA states that encryption devices for use in our governmental communications must operate securely for several decades to insure: (1) certification of the encryption scheme; (2) operation in the field; and (3) immunity for some time beyond their removal from the field. Moreover, the political costs of losing the security of our own communications, or our ability to collect foreign intelligence, could be staggering and probably not subject to financial measures. The NSA, in view of these national security implications, feels that university research on public cryptology should be controlled through prepublication reviews.

In the case of VLSI, the governmental concerns center on the leakage of this critical technology through foreign scholars, as well as through the unconstrained publication of research results. Since approximately one third of the engineering graduate students of our major universities are not U.S. citizens, the fears appear to rest on a sound numerical basis. Since VLSI circuits are used in a large variety of applications, including the control and instrumentation of weapons, the Government fears that we are weakening through such a leakage of technology the military strength of the U.S.

In addition, the easy export of forefront VLSI research gives an unfair commercial advantage to the international competition. In blunt terms, the Government asks why we freely export precious technology, while paying dearly for foreign imports such as oil and cars.

5.3 The Problems of Constrained Research

The imposition of constraints on research invariably results in a loss of effectiveness. Progress is slower and fewer people, hence fewer good people, are attracted to pursue such research. In addition, certain future opportunities are foreclosed and results that would have otherwise been achieved by a wider, intercommunicating community are either never realized or postponed.

The inherent coupling of research and education in our universities means that constraints on the former necessarily lead to constraints on the latter. As a result, in such a constrained environment we cannot train as effectively the scientists and engineers who after moving to industrial and academic settings will generate this nation's future technological progress.

In addition, and from a geo-political viewpoint, the control of U.S. research in certain critical technologies will tend to weaken our allies and is likely to lead third-world and neutral countries away from the U.S., toward possibly adversary countries for the acquisition of needed technology.

The imposition of constraints on foreign scholars who participate in U.S. university research will lead to reduction of the effective research workforce, since a large number of researchers, hence of good researchers, are not U.S. citizens. In addition, such restrictions will reduce the number of foreign scholars who acquire a first-hand knowledge of our system—a loss for the U.S., whether such scholars stay in this country or return to their own countries. In addition, the exclusion of foreign scholars from certain research activities is impracticable and creates an unpleasant climate. Impracticable because it is difficult for a university which is predicated on the free pursuit of ideas to police who pursues what ideas, and unpleasant because of the evident discrimination associated with such a restriction.

Finally, in today's setting of multinational corporations, it is not at all clear that control of university research or of its access by foreign scholars will be effective in reducing the overall leakage of critical technologies.

Taken together, these consequences suggest that such constraints are likely to reduce our overall technological leadership and weaken the very strength that they are intended to protect.

6. RECOMMENDED MIT POLICY

6.1 Introduction

The arguments of the preceding section have led us to search for effective means that can allay governmental concerns while preserving the fundamental strength of unconstrained research. There is clearly no perfect solution that can thoroughly satisfy both sides of this conflict. Accordingly, we have approached this serious problem with a degree of flexibility and a tolerance for less than perfect solutions.

The balance on which we have settled is embodied in our recommendations for a relevant MIT policy which is presented next along with a summary of our rationale.

6.2 Recommended MIT Policy

We believe that one important part of MIT's mission is to prepare our society for a technologically advanced future. To do this, we must continue to pursue leading-edge research in areas that we believe to be of future significance, and to prepare the future professionals in forefront technologies. Current and expected developments in communication, information systems and other areas of science and technology call for continued intensive research and development efforts on our part. In some areas, e.g., very large scale integrated circuit design (VLSI), continued academic involvement is also central to the evolution of the underlying disciplines, in this case electrical engineering and computer science. At the same time, serious concern has been expressed about some technology transfer resulting from normal university activities in these areas. We therefore believe it necessary to state our policy with respect to this issue.

Freedom of inquiry and freedom to communicate are essential features of a university. Accordingly, we must be able to teach and perform research in an atmosphere where ideas are freely pursued and exchanged. MIT's role in advancing technology should continue in this open atmosphere. It is also true we believe, that scientific and technological progress are best secured in an open atmosphere, and that the scientific costs to the nation of imposing restrictions outweigh the benefits. Openness also requires that as a general policy MIT not undertake classified research, or research whose results may not be freely published without prior permission. We believe that openness of the university also requires that, once they are among us, foreign students, faculty and scholars should be on an equal basis with their U.S. counterparts in their access to MIT academic and research projects. Moreover, restrictions on access to ideas or places within a university are difficult to enforce and likely to be ineffective.

Exceptions to these policies regarding publication, classification and foreign students and scholars may be made, but only in those very rare instances where the area of work is crucially important to MIT's educational mission and the exception is demonstrably necessary for the national good. If these conditions are not met, MIT will decline or discontinue the activity and, if appropriate, propose it for consideration off-campus or elsewhere.

MIT, like other universities, has a responsibility to the national interest. When sensitive but unclassified research at MIT is important to the national security we will take appropriate steps to ensure that the relevant government agencies are informed of the results. For example, it is our current policy to inform the U.S. Government of research in information protection and authentication by sending prepublication material in this area to the NSA at the same time that we send it to our close colleagues for technical comment. As a further example, we have also agreed with the NSF that in those rare instances in which we believe that certain of our cryptology research results require classification, we will submit them for review to the cognizant government agency prior to dissemination.

Government officials are urged to recognize the concern that bureaucratic forces are likely to try to convert exceptional circumstances into rules. We urge them to resist such forces.

6.3 Relationship of MIT Policy to the Corson Report

In view of the significance of the Corson Report, (see Section 3.7) and the similarity of the issues and recommendations addressed by both the Corson and MIT reports we make the following comments:

We are in full agreement with the principles of the Corson Report. Our concerns stem from the possible misinterpretation of the Report's specific criteria under which "gray area" research may be subject to restrictions and of its specific methods for implementing such restrictions. In particular, we fear that its detailed recommendations may be interpreted and implemented in ways which ignore their accompanying qualifications. If indeed such qualifications are ignored, the Corson Report recommendations could be read as restrictive imperatives.

Our own policy in Section 6.2 above calls for openness of communication and equality among foreign nationals and their U.S. peers. "Exceptions...may be made but only in those very rare instances where the area of work is crucially important to MIT's educational mission and the exception is demonstrably necessary for the national good." By not specifying, ***a priori***, the criteria for or the general nature of such exceptions, we feel that the danger of converting qualified examples into rules is mitigated.

Appendix A
COMMITTEE ON THE CHANGING NATURE OF INFORMATION
Membership

Richard B. Adler (since May 1981)
MIT Associate Department Head for Computer Science and Electrical Engineering

Michael L. Dertouzos, (Chairman)
Director, MIT Laboratory for Computer Science

John M. Deutch
Dean, MIT School of Science

George H. Dummer (since May 1981)
Director, MIT Office of Sponsored Programs

Professor Herman N. Eisen (since April 1982)
Professor of Immunology
MIT Department of Biology

Carl B. Feldbaum (through May 1981)
Attorney, Palomar Corporation

Francis E. Low (ex-officio)
MIT Provost

Jeffrey A. Meldman
Senior Lecturer in MIT Sloan School of Management

Associate Dean, Office of Dean for Student Affairs

Louis Menand, III
MIT Special Assistant to the Provost
Senior Lecturer in MIT Department of Political Science

Robert C. Merton (through October 1981)
Professor of Management
MIT Sloan School of Management

Ronald L. Rivest
Professor of Computer Science
MIT Department of Electrical Engineering and Computer Science

Walter A. Rosenblith
Institute Professor and Past MIT Provost

Kenneth A. Smith (ex-officio since July 1981)
MIT Associate Provost and
Vice President for Research

Robert E. Sullivan
Partner, Herrick and Smith

Judith J. Thomson
Professor of Philosophy
MIT Department of Linguistics and Philosophy

Gerald L. Wilson (since April 1982)
Dean, MIT School of Engineering

APPENDIX B
THE FIVE PRESIDENTS' LETTER

The Five Presidents' Letter

February 27, 1981

The Honorable Malcolm Baldrige
Secretary of Commerce
14th Street
Washington, D.C. 20230

The Honorable Alexander M. Haig, Jr.
Secretary of State
2201 C Street, N.W.
Washington, D.C. 20520

The Honorable Caspar Weinberger
Secretary of Defense
The Pentagon
Washington, D.C. 20301

Dear Mssrs. Baldrige, Haig, and Weinberger:

We are writing to request clarification of the applicability of certain export restrictions to teaching and research activities conducted by American universities. We are deeply concerned about recent attempts to apply to universities the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). Examples of such efforts by government agencies include a December 12, 1980, memorandum by the Director of the Very High Speed Integrated Circuit (VHSIC) Program Office, attempts to restrict publication of unclassified university research results arising from DOD-sponsored projects, and a Department of Commerce mandate to at least one university barring certain foreign scholars from that university's sponsored research activities due to their citizenship. Unfortunately, these initiatives appear to be only the first of many such actions to follow.

The ITAR and EAR regulations have existed for a number of years, and have not until now been applied to traditional university activities. The new construction of these regulations appears to contemplate government restrictions of research publications and of discourse among scholars, as well as discrimination based on nationality in the employment of faculty and the admission of students and visiting scholars. In the broad scientific and technical areas defined in the regulations, faculty could not conduct classroom lectures when foreign students were present, engage in the exchange of information with foreign visitors, present papers or participate in discussions at symposia and conferences where foreign nationals were present, employ foreign nationals to work in their laboratories, or publish research findings in the open literature. Nor could universities, in effect, admit foreign nationals to graduate studies in those areas. Such restrictions would conflict with the fundamental precepts that define the role and operation of this nation's universities.

The regulations could be interpreted to cover instruction and research which, although potentially useful in military applications, have much broader utility in such other areas as medical systems and communication equipment. Such interpretations of the regulations, coupled with their severe criminal penalties, could have a very real and unintended chilling effect of legitimate academic exchange.

Restricting the free flow of information among scientists and engineers would alter fundamentally the system that produced the scientific and technological lead that the government is now trying to protect and leave us with nothing to protect in the very near future. The way to protect that lead is to make sure that the country's best talent is encouraged to work in the relevant areas, not to try to build a wall around past discoveries.

It should be recognized that the only realistic way to "contain" VHSIC research is to classify the whole program. In our view this would be a self-defeating effort: the science underlying high technologies cannot be put back into the bottle. Furthermore, most universities have concluded that performance of classified research is incompatible with their essential purposes. University scientists would prefer, for the most part, to change their field of interest rather than have their research and teaching so constrained. Forcing high technology research out of universities would decrease our nation's competitive position, since the research would have to be carried out more slowly and less effectively in a classified atmosphere. Moreover, we would foreclose a continuous flow of new graduates from the university programs which have been flourishing up to this point. Elimination of such teaching and research from academic laboratories would endanger the future of graduate programs in engineering, computer science, and related fields, and would result in a tremendous loss of potential high technology otherwise available to American Industry. The new restrictions

represent the worst possible direction: they fail to protect the *status quo* and virtually guarantee that there will be no future.

Moreover, application of export restrictions to universities would pose significant practical difficulties. It would be virtually impossible for most universities to administer such restrictions given the necessarily decentralized and fluid nature of most campuses. Because it is so inconsistent with their character, universities are neither structured nor staffed to police the flow of legitimate visitors to a given laboratory or the dissemination of information by their faculty at international conferences, or, indeed, even in a campus classroom where foreign students happen to be present.

The December 12, 1980, memorandum mentioned earlier pertaining to the VHSIC Program assumes basic research can be differentiated from areas such as device design and fabrication techniques, process equipment, and software, for which approval of publication or presentation normally would be denied. Such distinctions are proposed to be made by government employees, using criteria of questionable reliability and suitability.

There is no such easy separation in any engineering curriculum intended to be relevant to our national industrial needs and problems. Furthermore, producing graduates with no "hands-on" experience in these areas would be of little value to American high technology industries.

The proposed extension of the restrictions to university activities ought not be made without a thorough assessment of the policy implications, the necessity and prospective effectiveness of the restrictions, the extent of disruption of the established role and operations of universities, and the serious legal and constitutional questions raised.

In the interim, it might be mutually advantageous for DOD to continue (selectively and sparingly) to rely on its classified research facilities to carry out the most sensitive segments of the VHSIC program. That has been its practice in previous years, and is far preferable to the application of these restrictive and virtually unenforceable regulations to universities. For those university activities which remain unclassified, we urge the government to cease all attempts to apply the restrictions until the broader issues are resolved.

We hope that after examining this issue carefully, you will clarify what has always been our understanding—namely, that the regulations are not intended to limit academic exchange arising from unclassified research and teaching.

Sincerely yours,

Donald Kennedy
President, Stanford University

Marvin L. Goldberger
President, California Institute of Technology

Paul E. Gray
President, Massachusetts Institute of Technology

Frank H. T. Rhodes
President, Cornell University

David S. Saxon
President, University of California